

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA

v.

Case No. 24-CR-50-JDP

STEVEN ANDEREGG,

DEFENDANT.

GOVERNMENT’S BRIEF IN SUPPORT OF DETENTION

The United States of America, by and through undersigned counsel, hereby submits this brief in support of its request under 18 U.S.C. § 3142(e) and (f) for the Court to order the defendant detained pending trial.

The defendant is charged in a four-count indictment with producing, distributing, and possessing obscene visual depictions of minors engaged in sexually explicit conduct and transferring obscene material to a minor under the age of sixteen. These charges stem from his use of generative artificial intelligence (“GenAI”) to create hyper-realistic images of nude and semi-clothed prepubescent children lasciviously exhibiting or touching their genitals or engaging in sexual intercourse. The defendant was caught by law enforcement after boasting to a fifteen-year-old about creating these images using a GenAI model called Stable Diffusion (produced by Stability AI) and sending the minor images of prepubescent boys displaying their erect penises in direct messages on Instagram. But this is not the defendant’s first encounter with law enforcement for suspected online child-exploitation crimes, nor are these the only criminal charges involving the

exploitation of minors pending against him. For these reasons, and as further explained below, the defendant poses a significant danger to this community and a risk of non-appearance, and this Court should find that there are no conditions of release that can adequately mitigate these risks.

I. FACTUAL BACKGROUND

In November 2023, law enforcement in Wisconsin received two CyberTips from the National Center for Missing and Exploited Children (“NCMEC”) related to a particular Instagram account (the “Subject Account”). The CyberTips advised that the user of the Subject Account sent AI-generated images of naked minors over Instagram Direct Messenger (“DM”) to a potential minor in October 2023. Instagram DM is an in-app messaging feature that allows an Instagram user to share and privately exchange text and images with one or more other users of Instagram.

After receiving these CyberTips, law enforcement obtained the contents of the Subject Account pursuant to a warrant. A review of this material revealed that, in September 2023, the user of the account posted an Instagram story consisting of a realistic GenAI image of minors wearing BDSM-themed leather clothes and a message encouraging others to “[c]ome check out what [they] are missing” on Telegram, which is an encrypted mobile-messaging application. Additionally, in the Subject Account’s direct messages on Instagram, the user discussed his desire to have sex with prepubescent boys and the fact that he has a wife and child and lives in Wisconsin. In one direct-message exchange, another user asked the Subject Account for nude images of minors and the Subject Account user advised that he has “tons” of images like that on Telegram before

sending this other user a Telegram link. And in other direct-message chats, the user of the Subject Account explained that he does not publicly post fully nude images of minors on Instagram because that would be illegal and discussed how he evades the detection of GenAI models that censor the production of sexually inappropriate content.

Law enforcement also located the Subject Account's direct-message conversation with a potential minor that was reported in the CyberTips. A review of this conversation confirmed that, in response to questioning from the Subject Account, the other user advised that he was only fifteen years old, which law enforcement has since verified was true. The user of the Subject Account then explained to the minor how he creates GenAI images by inputting text prompts in a text-to-image GenAI model called Stable Diffusion, which generates images based on his parameters. After asking if the minor would like any customized GenAI images, the user of the Subject Account sent a series of realistic images of semi-clothed minor boys, including three images that depict prepubescent boys graphically displaying their erect penises.

Based on the information provided by Instagram, law enforcement linked the Subject Account to an internet account under the defendant's name at his home in Holmen, Wisconsin. But this was not the first time that the defendant's internet account had been flagged during a child-exploitation investigation. Roughly four years prior, law enforcement had observed that someone using the internet at his home was requesting to download multiple files of known child sexual abuse material over an online peer-to-peer network. Law enforcement searched the defendant's home in furtherance of this investigation in 2020, during which the defendant admitted to using and deleting the

specific peer-to-peer program and often resetting his internet modem. No charges have been brought in connection with this prior investigation.

In February 2024, law enforcement obtained and executed a warrant to search the defendant's home in furtherance of its investigation of the Subject Account. The defendant voluntarily agreed to speak with law enforcement during the search and admitted to being familiar with Stable Diffusion before ending the interview. Law enforcement located his home office in the basement of the residence and found a work computer for his job as a software engineer¹ and his personal laptop. Law enforcement seized this personal laptop and two cell phones, among other devices, pursuant to the warrant. A review of these devices uncovered evidence linking the defendant to the Subject Account. Further, the review confirmed that the defendant installed Stable Diffusion, along with a graphical user interface and special add-ons created by other Stable Diffusion users that specialized in producing genitalia, on his personal laptop and then used these combined tools to generate photo-realistic images of minors. He had on this laptop over 13,000 GenAI images, with hundreds – if not thousands – of these images depicting nude or semi-clothed prepubescent minors lasciviously displaying or touching their genitals. Still others depict prepubescent minors touching what appear to be adult male penises or engaging in sexual intercourse. Additional evidence from the laptop indicates that he used extremely specific and explicit prompts to create these images. He

¹ A copy of the defendant's CV indicates that he has worked as a software engineer since 2003 and studied computer science in college. His CV also lists a recent job at a startup in which he "[u]tilize[d his] excellent technical understanding in formulating AI models" to develop the company's infrastructure.

likewise used specific “negative” prompts—that is, prompts that direct the GenAI model on what not to include in generated content—to avoid creating images that depict adults.

Following the search of his residence and additional investigation, the defendant was charged in La Crosse County Circuit Court with exposing a child to harmful material, in violation of Wis. Stat. § 948.11(2)(a), and first-degree sexual assault of a child under the age of thirteen, in violation of Wis. Stat. § 948.02(1)(e). *See State of Wisconsin v. Steven A. Anderegg*, Case No. 2024CF000185. He is currently released on bond in that case.

II. LEGAL STANDARD

The United States requests a detention hearing because the defendant has been charged with a felony that “involves a minor victim.” 18 U.S.C. § 3142(f)(1)(E). Pursuant to § 3142(g), the Court must determine whether there are any “conditions of release that will reasonably assure [his] appearance ... as required and the safety of any other person and the community.” When making this determination, the Court should consider (1) the nature and circumstances of the offense, (2) the weight of the evidence, (3) the defendant’s history and characteristics, and (4) the nature and seriousness of the danger to the community posed by the defendant’s release. *See* 18 U.S.C. § 3142(g). The government bears the burden of proving that the defendant is a risk of flight by a preponderance of the evidence and that he is a danger to the community by clear and convincing evidence. *See United States v. Portes*, 786 F.2d 758, 764-65 (7th Cir. 1985).

III. ARGUMENT

Based on careful consideration of the factors enumerated in 18 U.S.C. § 3142(g), the United States submits that there is no condition or combination of conditions that will

reasonably assure the safety of the community or the defendant's appearance should he be released pending trial.

A. The Nature and Circumstances of the Offense Charged

Starting first with the nature and circumstances of the offenses, the alleged conduct is exceptionally serious. Under the Sentencing Guidelines, if convicted of all offenses and given his other relevant conduct and the potential applicability of an enhancement for using his special skill in GenAI, the defendant's recommended sentencing range may be as high as life imprisonment. And while he has not been charged with a child-pornography offense under Chapter 110 of the United States Code—and thus avoids the rebuttable presumption in favor of detention in the Bail Reform Act, *see* 18 U.S.C. § 3142(e)(3)(E)—the defendant's conduct nevertheless implicates the very concerns that motivated Congress to apply this rebuttable presumption to this category of offenders through the Adam Walsh Act in the first place. *See* Adam Walsh Child Protection and Safety Act of 2006, Pub. L. No. 109-248, 120 Stat 587 (2006). Indeed, the images that the defendant produced are extremely realistic and clearly designed both to vividly depict minors engaged in sexually explicit conduct and arouse offenders who derive sexual gratification from seeing minors being exploited and abused.

Nor is the defendant's conduct limited to merely possessing these images. To the contrary, as detailed above, he actively cultivated an online community of like-minded offenders—through Instagram and Telegram—in which he could show off his obscene depictions of minors and discuss with these other offenders their shared sexual interest in children. Put differently, he used these GenAI images to attract other offenders who

could normalize and validate his sexual interest in children while simultaneously fueling these offenders' interest—and his own—in seeing minors being sexually abused.

And perhaps most concerning of all, the defendant distributed these images to a minor using an Instagram account that was plainly designed to allow the defendant to act on his sexual interest in children. When this minor made his age known, the defendant did not rebuff him or inquire further. Instead, he wasted no time in describing for this minor how he creates sexually explicit GenAI images and sent the child custom-tailored content. This conduct was not aimed at fostering a conversation about human anatomy or even artificial intelligence—rather, the only reasonable explanation for sending these images was to sexually entice the child. And as a result of this exceptionally serious conduct, the defendant now faces a mandatory minimum sentence of five years and a maximum sentence of decades in prison if convicted.

B. The Weight of the Evidence

The weight of the evidence against the defendant is strong. The Instagram account used to distribute the sexually explicit images has been linked directly to the defendant and his home, and the direct messages sent by the user further corroborate that the account belonged to him. A trove of similar GenAI images was recovered from the defendant's personal laptop in his home office, as well as his cell phone. The defendant also told law enforcement that he is familiar with the specific GenAI model used to create these images, and even has professional experience working with AI.

C. The History and Characteristics of the Defendant

While the defendant has no prior criminal convictions, his offense conduct was not an isolated incident. Rather, it was part of a long-standing and ongoing course of conduct for which he has evaded accountability until very recently. Indeed, just a few years ago, law enforcement searched his home after observing that someone was attempting to download child sexual abuse material over a peer-to-peer network. And even assuming that there is an innocent explanation for this—which, to be sure, is a dubious supposition given what the current investigation has revealed—the prior search should have signaled to the defendant that law enforcement takes seriously investigations that uncover evidence of possible child exploitation. Yet less than five years later, law enforcement had to return to the defendant’s home after learning that he was sending sexually explicit imagery to a minor over Instagram. On top of that, he is now facing charges in La Crosse County Circuit Court for separate criminal conduct involving the sexual assault of a child under the age of thirteen that was only recently uncovered through and as a result of this investigation.

D. The Nature and Seriousness of the Danger to the Community that Would Be Posed by the Defendant’s Release

The danger the defendant poses to the community is immense. As noted *supra*, despite having no prior convictions, the evidence indicates that his criminal conduct extends well beyond the scope of the current charges. And, as best the government can tell, all of this conduct has been motivated by a sexual interest in children. Accordingly, if he were to reoffend while on pretrial release, not only would the harm caused by such

recidivist conduct likely be severe, but it would be inflicted on the most vulnerable members of his community – minor children.

To make matters worse, the defendant is extremely technologically savvy. He studied computer science and has decades of experience in software engineering. While computer monitoring may address the danger posed by less sophisticated offenders, the defendant's background provides ample reason to conclude that he could sidestep such restrictions if he decided to. And if he did, any reoffending conduct would likely go undetected. Indeed, despite the scope of his apparent crimes, the defendant was only caught because Instagram detected and reported that he sent a fifteen-year-old boy obscene images of minors engaged in sexually explicit conduct by direct message on a single day in October 2023. Since October 2023, Meta has begun to roll out default end-to-end encryption on its Facebook and Messenger platforms and has indicated that Instagram's direct message feature would follow soon after.² If default end-to-end encryption were enabled on Instagram, it is highly likely that no one, including Meta, would be able to detect what the defendant might send by direct message except for the recipient of that message. The same goes for Telegram, which the defendant discussed using with others, and any number of other encrypted messaging applications. And while AI companies have pledged to make it more difficult for offenders to use future

² See End-to-end encryption on Instagram, https://help.instagram.com/936296650678728/?helpref=related_articles (last visited May 16, 2024).

versions of GenAI tools to generate images of minors being sexually abused,³ such steps will do little to prevent savvy offenders like the defendant from running prior versions of these tools locally from their computers without detection.

IV. CONCLUSION

Given the serious nature of the defendant's conduct and the penalties he faces if convicted, there are no conditions that would ensure his appearance in court or the protection of the community if he were to be released. Accordingly, the defendant should be detained pending trial pursuant to 18 U.S.C. § 3142(e). If the Court disagrees, the United States submits that the defendant should, at a minimum, be subject to computer and GPS monitoring and prohibited from having any contact with minors.

Dated this 20th day of May, 2024.

Respectfully submitted,

STEVEN J. GROCKI
Chief, Child Exploitation & Obscenity Section

By:

/s/ William G. Clayman
William G. Clayman
Trial Attorney

³ See Kat Tenbarge, *Top AI companies commit to child safety principles as industry grapples with deepfake scandals*, NBC News (April 23, 2024, 8:09 PM EDT), <https://www.nbcnews.com/tech/tech-news/top-ai-companies-commit-child-safety-principles-thorn-rcna148988>.